

Program Overview



We seek to serve as a bridge from inspiration to implementation by combining innovations in science and engineering with insights gained through end-to-end systems studies of threat scenarios.

These activities reside within the Non-proliferation, Arms Control, and International Security Directorate (NAI) and the Homeland Security Organization (HSO) at the Lawrence Livermore National Laboratory.

Our primary customers are the Department of Energy, the Department of Defense and the Department of Homeland Security.

Information Analysis and Infrastructure Protection

Lawrence Livermore National Laboratory

The goal of the Lawrence Livermore National Laboratory's Information Analysis and Infrastructure Protection Program (IAIP) is to comprehensively understand the threat posed by terrorists to US critical infrastructure and key assets in order to inform local, regional, state, and federal protection efforts.

Background

As a DOE national security laboratory, LLNL has a long history of supporting threat analysis of nuclear, chemical, biological, cyber and explosive threats.

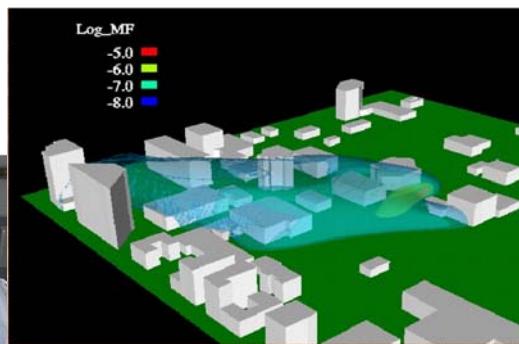
LLNL's International Assessments program has conducted analysis of threats to the nation for almost 40 years and provides important input to policy makers as they develop strategies for U.S. responses to events affecting national and international security.

We apply our scientific and engineering expertise toward analyzing vulnerabilities and risks of national critical infrastructure including: oil, gas, electricity, water, transportation, finance, cyber national icons, and telecommunications. Our analysis efforts have resulted in widely used methodologies for assessing risk and developing countermeasures for protection. LLNL operates the Department of Energy's Computer Advisory Center (CIAC) for cyber attack alert and warning across the DOE complex. CIAC develops tools and techniques for cyber defense and is exemplary of an operational effort for homeland security that is continuously enhanced by technology development.

Recently the Homeland Security mission has provided a focused opportunity for us to integrate our tools and analytical capabilities to comprehensively understand the threat spectrum and link that knowledge to infrastructure vulnerabilities in order to assist decision makers mitigate risks. Threat integration is the cornerstone to LLNL's approach to helping secure the national infrastructure.

Our IAIP efforts are focused on two key areas:

- the development of analytic expertise and tools to support an integrated threat-vulnerability analysis capability;
- science and technology applied to the development and evaluation of countermeasures for the protection of critical infrastructure.



Lawrence Livermore National Laboratory

Key Focus areas

LLNL's IAIP efforts are supported by four key areas.

Threat Assessments

LLNL's analysts provide a comprehensive, all-source analytic capability focused on identifying and characterizing WMD capabilities of states, groups, or individuals in direct support of other development efforts aimed at mitigating the potential impact of such identified threats against US citizens, property or interests.

Infrastructure Protection

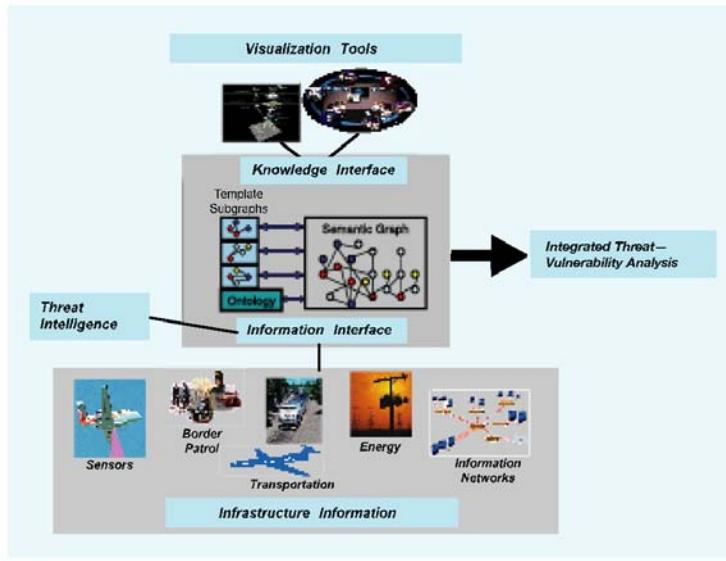
LLNL's expertise in applied engineering and physical sciences, advanced scientific computing, information technologies and systems science provide a strong foundation for analysis of risks and vulnerabilities associated with critical infrastructure. We are supporting federal, state and local government as well as private industry efforts to characterize risks to the infrastructure and to develop operational and strategic options for mitigating risks. We are working directly with infrastructure owners and operators to understand their operational issues and constraints so that realistic countermeasures can be developed and deployed.

Threat Vulnerability Integration System (TVIS)

TVIS will result in a fully operational system for large-scale information fusion based on leading edge technology developed in partnership between the US government, industry and the national laboratories. Its objective is to provide DHS and other analysts with the ability to perform rapid and effective threat-vulnerability mapping and warning. TVIS is developing and enabling state-of-the-art analytic tools and techniques in data mining, data fusion, semantic graphs and visualization to assist analysts identify previously unknown linkages and associations.

Advanced Scientific Computing (ASC)

The ASC, a national research program in scalable, integrated information and simulation science is providing the integrating platform required to serve the IAIP mission. The LLNL ASC program is developing scalable algorithms and software for information management and knowledge discovery to support threat identification and vulnerability linkages. It is also developing scalable integrated simulation analysis capabilities for use in vulnerability and risk assessment for protecting infrastructure and incident management.



For more information,
contact:
Wes Spain
Phone: (925) 422-0261
Fax: (925) 422-4100
E-Mail: spain1@llnl.gov
M1052-04

